

I	{0 0}	{0 1}	{1 0}	{1 0}
				Q
	00	01	03	02
	10	11	13	12
	30	31	33	32
	20	21	23	22
				(10)

Figure 1

	01	02
10	13	
	31	32

Figure 2

remove the most protected bit of I

```
I-value {}      I      {0}{1}{1}{0}
Q-value ()           01   00
                      10   11
                      31   30
                     20   21
                           Q
                           (00)
                           (01)
                           (11)
                           (10)
```

Figure 3

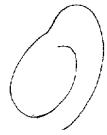
```
01-----00
10---|---11  |
| 31---|---30
20---|---21
```

Figure 4

remove the least protected bit of I

I-value	{ }	I	{ 0 } { 0 } { 1 } { 1 }
Q-value	()		Q
		00	(00)
		10	(01)
		30	(11)
		20	(10)
		31	
		21	

Figure 5



00-----01
10---|-11 |
| 30---|-31 |
20-----21

Figure 6

remove the most protected bit of Q

I-value { }	I	{0 {1 {1 {0
Q-value ()		0} 0} 1} 1}
		Q
	10	02
		13
	00	12
		03
		11
		(0)
		(1)
		(1)
		(0)

Figure 7

02-----01
10-----13 |
| 12-----11
00-----03

Figure 8

remove the least protected bit of Q

I-value	{}	I	{0}	{1}	{1}	{0}
Q-value	{}	Q	{0}	{0}	{1}	{1}
			02	01		
			00	03		
			12	11		
			10	13		

Figure 9

02----01
00--|-03 |
| 12--|-11
10----13

Figure 10.

0	0	0	0	1	1	1	1
0	0	1	1	1	0	0	
0	1	1	0	0	1	1	0
00	01	03	02	06	07	05	04
10	11	13	12	16	17	15	14
30	31	33	32	36	37	35	34
20	21	23	22	26	27	25	24
60	61	63	62	66	67	65	64
70	71	73	72	76	77	75	74
50	51	53	52	56	57	55	54
40	41	43	42	46	47	45	44

Figure 11

01	02	07	04
10	13	16	15
31	32	37	34
20	23	26	25
70	61	62	67
51	73	76	75
40	43	52	57

Figure 12

remove the most protected bit of I

Figure 13

01-----02-----03-----00
10-- -13-----12-----11 -
31 32 33 30
20 23 22 21 -
61 62 63 60
70 73 72 71 -
51 52 53 50
40-----43-----42-----41

Figure 14

remove the second most protected bit of I

I-value	{}	I	{0 0} 1}	{0 1} 0}	{1 0} 0}	{1 1} 1}	{1 1} 0}	Q
I-value	{}							
Q-value	()							
		01	00	03	02	(000)		
10		11	12	13		(001)		
		31	30	33	32	(011)		
20		21	22	23		(010)		
		61	60	63	62	(110)		
70		71	72	73		(111)		
		51	50	53	52	(101)		
40		41	42	43		(100)		

Figure 15

01-----00-----03-----02
10-----11-----12-----13
31 30 33 32
20 21 22 23
61 60 63 62
70 71 72 73
51 50 53 52
40-----41-----42-----43

Figure 16

remove the least protected bit of I

Figure 17

00-----01-----03-----02
10-- -11-----13-----12
30 31 32
20 21 23 22
60 61 62
70 71 73 72
50-----51-----53-----52
40-----41-----43-----42

Figure 18

remove the most protected bit of Q

```
I-value {}      I      {0 {0 {0 {1 {1 {1 {1
    0 0 1 1 1 0 0
    0} 1} 1} 0} 0} 1} 1} 0} 0} 1} 0} 1} 0} 0} Q
Q-value ()
```

01	02	07	04	(00)
10	13	16	15	(01)
31	32	37	34	(11)
20	23	26	25	(10)
21	22	27	24	(10)
30	33	36	35	(11)
11	12	17	14	(01)
00	03	06	05	(00)

Figure 19

01-----02-----07-----04
10-- -13-----16-----15
31 32 37 34
20 23 26 25
21 22 27 24
30 33 36 35
11-----12-----17--- -14
00-----03-----06-----05

Figure 20

remove the second most protected bit of Q

```
I-value {}  

Q-value ()
```

01	02	07	04	(00)
10	13	16	15	(01)
11	12	17	14	(01)
00	03	06	05	(00)
21	22	27	24	(10)
30	33	36	35	(11)
31	32	37	34	(11)
20	23	26	25	(10)

Figure 21

01	02	07	04
10	13	16	15
11	12	17	14
00	03	06	05
21	22	27	24
30	33	36	35
31	32	37	34
20	23	26	25

Figure 22.

remove the least protected bit of Q

```
I-value {}
Q-value ()
I
  {0 {0 {0 {1 {1 {1 {1 {1
  0 0 1 1 1 0 0
  0} 1} 0} 0} 1} 1} 0} 0} Q
  01 02 07 04 (00)
  00 03 06 05 (00)
  11 12 17 14 (01)
  10 13 16 15 (01)
  31 32 37 34 (11)
  30 33 36 35 (11)
  21 22 27 24 (10)
  20 23 26 25 (10)
```

Figure 23

```
01-----02-----07-----04
00---|---03-----06-----05 |
| 11 12 17 14
10 | 13 16 15 |
| 31 32 37 34
30 | 33 36 35 |
| 21-----22-----27---|-24
20-----23-----26-----25
```

Figure 24

卷之三

Figure 25

10	01	02	07	04	0D	0E	0B	08
31	13	32	16	15	1C	1F	1A	19
20	23	26	37	34	3D	3E	3B	38
61	61	62	67	25	2C	2F	2A	29
70	73	76	75	64	6D	6E	6B	68
51	51	52	57	54	5D	5E	5B	58
40	43	46	45	4C	4F	4A	49	
C1	C2	C7	C4	CD	CE	CB	C8	
D0	D3	D6	D5	DC	DF	DA	D9	
F1	F2	F7	F4	FD	FE	FB	F8	
E0	E3	E6	E5	EC	EF	EA	E9	
A1	A2	A7	A4	AD	AE	AB	A8	
B0	B3	B6	B5	BC	BF	BA	B9	
91	92	97	94	9D	9E	9B	98	
80	83	86	85	8C	8F	8A	89	

Figure 26

remove the most protected bit of T

Figure 27

10	-	13	-	02	-	07	-	04	-	05	-	06	-	03	-	00
	31		32		37		34		35		36		33		30	
20		23		26		25		24		27		22		21		
	61		62		67		64		65		66		63		60	
70		73		76		75		74		77		72		71		
	51		52		57		54		55		56		53		50	
40		43		46		45		44		47		42		41		
	C1		C2		C7		C4		C5		C6		C3		C0	
D0		D3		D6		D5		D4		D7		D2		D1		
	F1		F2		F7		F4		F5		F6		F3		F0	
E0		E3		E6		E5		E4		E7		E2		E1		
	A1		A2		A7		A4		A5		A6		A3		A0	
B0		B3		B6		B5		B4		B7		B2		B1		
	91		92		97		94		95		96		93		90	
80		83		86		85		84		87		82		81		

Figure 28

remove the second most protected bit of I

```

I-value {} I
Q-value ()
```

01	02	03	00	05	06	07	04	(0000)
10	13	12	11	14	17	16	15	(0001)
31	32	33	30	35	36	37	34	(0011)
20	23	22	21	24	27	26	25	(0010)
61	62	63	60	65	66	67	64	(0110)
70	73	72	71	74	77	76	75	(0111)
51	52	53	50	55	56	57	54	(0101)
40	43	42	41	44	47	46	45	(0100)
C1	C2	C3	C0	C5	C6	C7	C4	(1100)
D0	D3	D2	D1	D4	D7	D6	D5	(1101)
F1	F2	F3	F0	F5	F6	F7	F4	(1111)
E0	E3	E2	E1	E4	E7	E6	E5	(1110)
A1	A2	A3	A0	A5	A6	A7	A4	(1010)
B0	B3	B2	B1	B4	B7	B6	B5	(1011)
91	92	93	90	95	96	97	94	(1001)
80	83	82	81	84	87	86	85	(1000)

1

Figure 29

01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
31	32	33	30	35	36	37	38	39	3A	3B	3C	3D	3E	3F	
20	21	22	21	24	27	26	25	28	29	2A	2B	2C	2D	2E	2F
61	62	63	60	65	66	67	68	69	6A	6B	6C	6D	6E	6F	
70	71	72	71	74	77	76	75	78	79	7A	7B	7C	7D	7E	7F
51	52	53	50	55	56	57	58	59	5A	5B	5C	5D	5E	5F	
40	41	42	41	44	47	46	45	48	49	4A	4B	4C	4D	4E	4F
C1	C2	C3	C0	C5	C6	C7	C8	C9	C0A	C0B	C0C	C0D	C0E	C0F	
D0	D3	D2	D1	D4	D7	D6	D5	D8	D9	D0A	D0B	D0C	D0D	D0E	D0F
F1	F2	F3	F0	F5	F6	F7	F8	F9	F0A	F0B	F0C	F0D	F0E	F0F	
E0	E3	E2	E1	E4	E7	E6	E5	E8	E9	E0A	E0B	E0C	E0D	E0E	E0F
A1	A2	A3	A0	A5	A6	A7	A8	A9	A0A	A0B	A0C	A0D	A0E	A0F	
B0	B3	B2	B1	B4	B7	B6	B5	B8	B9	B0A	B0B	B0C	B0D	B0E	B0F
91	92	93	90	95	96	97	98	99	90A	90B	90C	90D	90E	90F	
80	83	82	81	84	87	86	85	88	89	80A	80B	80C	80D	80E	80F

Figure 30

remove the third most protected bit of I

I-value { } I
Q-value ()

α

01	00	03	02	07	06	05	04	(0000)
10	11	12	13	16	17	14	15	(0001)
31	30	33	32	37	36	35	34	(0011)
20	21	22	23	26	27	24	25	(0010)
61	60	63	62	67	66	65	64	(0110)
70	71	72	73	76	77	74	75	(0111)
51	50	53	52	57	56	55	54	(0101)
40	41	42	43	46	47	44	45	(0100)
C1	C0	C3	C2	C7	C6	C5	C4	(1100)
D0	D1	D2	D3	D6	D7	D4	D5	(1101)
F1	F0	F3	F2	F7	F6	F5	F4	(1111)
E0	E1	E2	E3	E6	E7	E4	E5	(1110)
A1	A0	A3	A2	A7	A6	A5	A4	(1010)
B0	B1	B2	B3	B6	B7	B4	B5	(1011)
91	90	93	92	97	96	95	94	(1001)
80	81	82	83	86	87	84	85	(1000)

Figure 31

01-----00-----03-----02-----07-----06-----05-----04
 10--|-11-----12-----13-----16-----17-----14-----15-----|
 | 31 30 33 32 37 36 35 34
 20 | 21 22 23 26 27 24 25 |
 | 61 60 63 62 67 66 65 64
 70 | 71 72 73 76 77 74 75 |
 | 51 50 53 52 57 56 55 54
 40 | 41 42 43 46 47 44 45 |
 | C1 C0 C3 C2 C7 C6 C5 C4
 D0 | D1 D2 D3 D6 D7 D4 D5 |
 | F1 F0 F3 F2 F7 F6 F5 F4
 E0 | E1 E2 E3 E6 E7 E4 E5 |
 | A1 A0 A3 A2 A7 A6 A5 A4
 B0 | B1 B2 B3 B6 B7 B4 B5 |
 | 91-----90-----93-----92-----97-----96-----95-----|
 80-----81-----82-----83-----86-----87-----84-----85-----|

Figure 32

remove the least protected bit of I

Figure 33

00	-	-01	-	-03	-	-02	-	-06	-	-07	-	-05	-	-04	
10	-	-11	-	-13	-	-12	-	-16	-	-17	-	-15	-	-14	
	30		31		33		32		36		37		35		34
20	-	21	-	23	-	22	-	26	-	27	-	25	-	24	-
	60		61		63		62		66		67		65		64
70	-	71	-	73	-	72	-	76	-	77	-	75	-	74	-
	50		51		53		52		56		57		55		54
40	-	41	-	43	-	42	-	46	-	47	-	45	-	44	-
	C0		C1		C3		C2		C6		C7		C5		C4
D0	-	D1	-	D3	-	D2	-	D6	-	D7	-	D5	-	D4	-
	F0		F1		F3		F2		F6		F7		F5		F4
E0	-	E1	-	E3	-	E2	-	E6	-	E7	-	E5	-	E4	-
	A0		A1		A3		A2		A6		A7		A5		A4
B0	-	B1	-	B3	-	B2	-	B6	-	B7	-	B5	-	B4	-
	90		91		93		92		96		97		95		94
80	-	81	-	83	-	82	-	86	-	87	-	85	-	84	-

Figure 34

remove the most protected bit of Q

```

I-value   { } I
Q-value   ()

```

01	02	07	04	0D	0E	0B	08	(000)
10	13	16	15	1C	1F	1A	19	(001)
31	32	37	34	3D	3E	3B	38	(011)
20	23	26	25	2C	2F	2A	29	(010)
61	62	67	64	6D	6E	6B	68	(110)
70	73	76	75	7C	7F	7A	79	(111)
51	52	57	54	5D	5E	5B	58	(101)
40	43	46	45	4C	4D	4F	4A	(100)
41	42	47	44	4D	4E	4B	49	(100)
50	53	56	55	5C	5F	5A	59	(101)
71	72	77	74	7D	7E	7B	78	(111)
60	63	66	65	6C	6F	6A	69	(110)
21	22	27	24	2D	2E	2B	28	(010)
30	33	36	35	3C	3F	3A	39	(011)
11	12	17	14	1D	1E	1B	18	(001)
00	03	06	05	0C	0F	0A	09	(000)

α

Figure 35

01	02	07	04	0D	0E	0B	08
10	13	16	15	1C	1F	1A	19
31	32	37	34	3D	3E	3B	38
20	23	26	25	2C	2F	2A	29
61	62	67	64	6D	6E	6B	68
70	73	76	75	7C	7F	7A	79
51	52	57	54	5D	5E	5B	58
40	43	46	45	4C	4F	4A	49
41	42	47	44	4D	4E	4B	48
50	53	56	55	5C	5F	5A	59
71	72	77	74	7D	7E	7B	78
60	63	66	65	6C	6F	6A	69
21	22	27	24	2D	2E	2B	28
30	33	36	35	3C	3F	3A	39
11	12	17	14	1D	1E	1B	18
00	03	06	05	0C	0F	0A	09

Figure 36

remove the second most protected bit of Q

Figure 37

01	02	07	04	0D	0E	0B	08
10	-13	-16	-15	-1C	-1F	-1A	-19
1	31	32	37	34	3D	3E	3B
20	23	26	25	2C	2F	2A	29
1	21	22	27	24	2D	2E	2B
30	1	33	36	35	3C	3F	3A
1	11	12	17	14	1D	1E	1B
00	1	03	06	05	0C	0F	0A
1	41	42	47	44	4D	4E	4B
50	1	53	56	55	5C	5F	5A
1	71	72	77	74	7D	7E	7B
60	1	63	66	65	6C	6F	6A
1	61	62	67	64	6D	6E	6B
70	1	73	76	75	7C	7F	7A
1	51	-52	-57	-54	-5D	-5E	-5B
40	1	-43	-46	-45	-4C	-4F	-4A
							-49

Figure 38

remove the third most protected bit of Q

Figure 39

01-----02-----07-----04-----0D-----0E-----0B-----08
10---|---13---|---16---|---15---|---1C---|---1F---|---1A---|---19
| 11 12 17 14 1D 1E 1B 18
00 | 03 06 05 0C 0F 0A 09 |
| 21 22 27 24 2D 2E 2B 28
30 | 33 36 35 3C 3F 3A 39 |
| 31 32 37 34 3D 3E 3B 38
20 | 23 26 25 2C 2F 2A 29 |
| 61 62 67 64 6D 6E 6B 68
70 | 73 76 75 7C 7F 7A 79 |
| 71 72 77 74 7D 7E 7B 78
60 | 63 66 65 6C 6F 6A 69 |
| 41 42 47 44 4D 4E 4B 48
50 | 53 56 55 5C 5F 5A 59 |
| 51---|---52---|---57---|---54---|---5D---|---5E---|---5B---|---58
40-----43-----46-----45-----4C-----4F-----4A-----49

Figure 40

remove the least protected bit of Q

8

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0G	0H	0I	0J	0K	0L	0M	0N	0O	0P	0Q	0R	0S	0T	0U	0V	0W	0X	0Y	0Z
10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	1G	1H	1I	1J	1K	1L	1M	1N	1O	1P	1Q	1R	1S	1T	1U	1V	1W	1X	1Y	1Z
20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	2G	2H	2I	2J	2K	2L	2M	2N	2O	2P	2Q	2R	2S	2T	2U	2V	2W	2X	2Y	2Z
30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	3G	3H	3I	3J	3K	3L	3M	3N	3O	3P	3Q	3R	3S	3T	3U	3V	3W	3X	3Y	3Z
40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	4G	4H	4I	4J	4K	4L	4M	4N	4O	4P	4Q	4R	4S	4T	4U	4V	4W	4X	4Y	4Z

Figure 41

01-----02-----07-----04-----05-----0C-----0D-----0E-----0B-----08
00-----|-----03-----06-----05-----0F-----0A-----09-----|
| 11 12 17 14 1D 1E 1B 18
| 10 13 16 15 1C 1F 1A 19 |
| 31 32 37 34 3D 3E 3B 38 |
30 | 33 36 35 3C 3F 3A 39 |
| 21 22 27 24 2D 2E 2B 28 |
20 | 23 26 25 2C 2F 2A 29 |
| 61 62 67 64 6D 6E 6B 68 |
60 | 63 66 65 6C 6F 6A 69 |
| 71 72 77 74 7D 7E 7B 78 |
70 | 73 76 75 7C 7F 7A 79 |
| 51 52 57 54 5D 5E 5B 58 |
50 | 53 56 55 5C 5F 5A 59 |
| 41-----42-----47-----44-----4D-----4E-----4B-----4B-----48 |
40-----43-----46-----45-----4C-----4F-----4A-----4A-----49 |

Figure 42

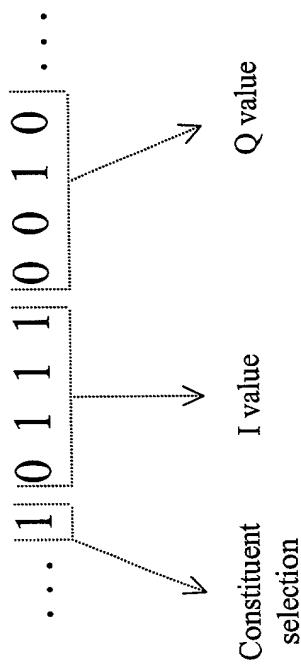


Figure 43

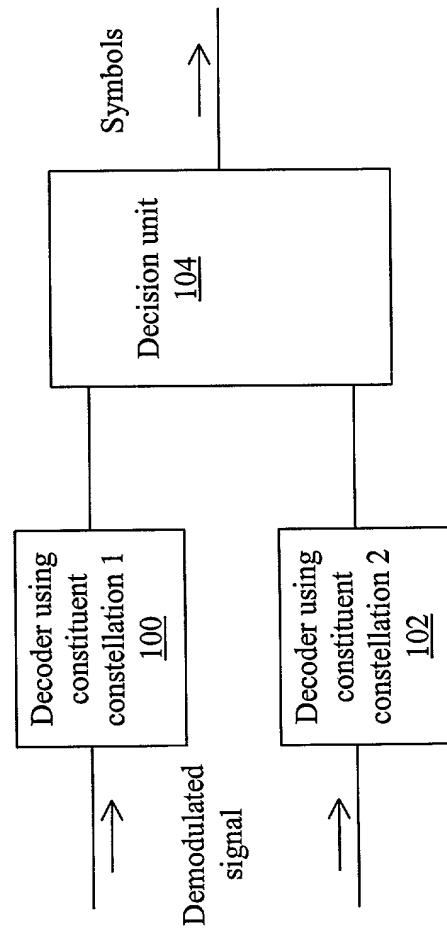


Figure 44